

### **REMARKS**

Claims 21-31 are pending. Claims 21-31 stand rejected. Claims 21, 22, 23, 25, 26, 27, 28, 29, 30, and 31 have been amended. Claims 21, 22, 25, 26, 27, 28, 29, 30, and 31 have been amended to make clear that the Applicant is not claiming in means-plus-function format. Applicants respectfully request reconsideration of the rejections in light of the amendments and arguments presented.

### **35 U.S.C. § 103 Rejections**

#### *Status*

Claims 21-31 stand rejected under 35 U.S.C. § 103 as being anticipated by Stenberg (International Publication No. WO 011/3666) in view of Rezaiifar et al. (U.S Patent Publication No. 2003/0055964).

#### *Cited Reference - Stenberg*

Stenberg describes a method for authenticating a mobile terminal in a hybrid network architecture formed by the combination of a TETRA network (radio access network layer) and a GSM network (overlying network layer). The authentication method enables the authentication of a user in a hybrid network architecture composed of *two layers* (the TETRA and the GSM network layers) that do not use the exact same authentication data. (Stenberg page 8 lines 8-9 and lines 26-29). However, the authentication parameters of the second authentication method *are derived from the authentication parameters of the first authentication*. (Stenberg page 18 lines 15-17 and lines 26-29). Thus, the authentications of Stenberg are not independent of each other.

#### *Cited Reference - Rezaiifar*

Rezaiifar describes authorization of an access terminal that has requested a particular service. If the terminal gets authorized, a Service Selector ("SS") selects a service provider based on the access terminal's capabilities. (Rezaiifar at para. 0036.) In this manner, Rezaiifar attempts to make the most out of the terminal's capabilities. Regarding authentication, Rezaiifar

discloses only conventional authentication, which makes sense because Rezaiifar is directed to getting the most out of the capabilities of a particular terminal, not simplifying authentication.

In Rezaiifar, authentication is performed by a conventional AAA server (not the SS). (Rezaiifar at Fig. 2 element 204 and para. 0036.) Once the terminal is authenticated, a service query is formatted. (Rezaiifar at para. 0040.) The service query includes a source address, a destination address, and the *terminal's capabilities*. (Rezaiifar at Fig. 2 element 212 and para. 0040.) A BSC/PCF receives the service query, and if it determines that the terminal is attempting to contact the SS for the first time, it sends a message to the SS. (Rezaiifar at para. 0042.) The SS then performs service *authorization in accordance with the attributes of the user's terminal*. (Rezaiifar at para. 0042.) If the service is authorized, the SS selects a service provider in accordance to the *terminal's capabilities*. As clearly shown in Figure 2, Rezaiifar discloses *only one authentication*, a conventional authentication, which is shown at element 204.

#### *Independent claims*

The independent claims include features neither disclosed nor suggested by the cited references, either alone or in combination, namely as represented by claim 21:

21. (Currently Amended) A method for authenticating a user for access to at least two entities of a data transmission network via a terminal, *each data entity having an associated authentication device, the authentication devices being independent of each other*, the method comprising:

- a random number is transmitted to the terminal,
- data for authenticating the user to the two entities of the network is calculated using at least one predefined cryptographic algorithm applied to the random number received and at least one secret key specific to the user,
- the terminal inserts, in an access request, data for identifying the user to said two entities of the network and the calculated authentication data, and transmits the access request to an access controller, wherein the inserted data for authenticating the user comprises a distinct set of data for each of the two entities;

- *the access controller transmits, to each of the authentication devices for the two entities, a respective authentication request* containing the identification data and the distinct set of inserted data for authenticating the user to the respective entity of the network, contained in the access request,

- the authentication devices servers of the entities carry out a user authentication procedure, on the basis of user identification and authentication data, contained in the authentication requests, and

- authentication reports containing results of the authentication procedures carried out by the authentication devices servers of each of said two network entities are transmitted to the terminal. (emphasis added)

Stenberg does not disclose or suggest authentication to "at least two entities of a data transmission network ... each data entity having an associated authentication device, the *authentication devices being independent of each other*," as recited by claim 21. In contrast, Stenberg's two networks use authentication algorithms that are related to each other in that authentication parameters in one authentication procedure are *derived* from authentication parameters in the other procedure. (Stenberg page 18 lines 15-17 and lines 26-29).

The problem being solved in Stenberg is quite different from the problem faced by the Applicants. Applicants did not try to streamline authentication procedures performed on two overlaid networks which have a derivation-based authentication scheme. Instead, Applicants' disclosure simplified the authentication of a terminal to *two distinct and independent entities* (e.g., two service providers like an Internet access provider and a bank website), rather than overlaid and related networks. The Applicants' disclosure can provide for authentication to two independent service providers at the same time with a single request from the user because the access controller is intelligent enough to transmit authentication requests to each of the service providers using the proper authentication procedure for those service providers. The two service providers can have separate and independent authentication procedures (which might happen to share common parameters, such as, username), rather than the derivation-based authentication procedures associated with the overlaid, related networks of Stenberg.

Stenberg also fails to disclose or suggest that "the *inserted data* for *authenticating* the user comprises a *distinct set of data for each of the two entities*," as recited by the claims. The

examiner notes this deficiency in Stenberg, and relies on Rezaiifar for such disclosure. Rezaiifar, however, does not cure this deficiency of Stenberg because Rezaiifar discloses authentication to *only a single entity*. Figure 2 of Rezaiifar clearly shows only a single authentication at element 204 – “Authentication (RADIUS).” While Rezaiifar does note elsewhere in its specification that the SS can perform a “service authorization,” this is not user authentication, nor is it related to user authentication . (Rezaiifar at para. 0042.) In fact, it is quite the opposite. Rezaiifar notes that “if the *service* is authorized, the SS...selects a service provider in accordance with the [terminal's] *capabilities*.” This is unrelated to whether the *user* can be authenticated.

Moreover, Rezaiifar does not describe an access controller which transmits to each of the *two entities*, a respective *authentication request* containing the identification data and the authentication data to the respective entity of the network contained in the access request. As clearly shown in Figure 2 of Rezaiifar, the Service Selector does not transmit *any* authentication requests.

Claims 25, 27, and 29, as amended, include similar features to those described above in connection with claim 21 and are patentable for similar reasons. Claims 22-24, 26, 28, and 30-31 each depend from one of independent claims 21, 25, 27, or 29, and are therefore allowable for at least the reasons given above. Applicants therefore respectfully request that the Examiner withdraw the rejections of claims 21-31.

### **CONCLUSION**

For all the foregoing reasons, Applicants respectfully submit that the application is in condition for allowance.


Applicant : Transy et al.  
Serial No. : 10/565,571  
Filed : August 2, 2006  
Page : 11 of 11

Attorney's Docket No.: 18394-  
0017US1 / RVL/PA61423US

Please apply the fees for a Request for Continued Examination and Extension of Time, along with any other charges or credits, to deposit account 06-1050 referencing attorney docket no. 18394-0017US1.

Respectfully submitted,

Date: June 17, 2009

  
\_\_\_\_\_  
Raymond N. Scott, Jr.  
Reg. No. 48,666

Fish & Richardson P.C.  
P.O. Box 1022  
Minneapolis, MN 55440-1022  
Telephone: (302) 652-5070  
Facsimile: (877) 769-7945